IN THE SPECIFICATION:

Page 10, line 23 through page 12, line 17:

Fig. 1 is a block diagram showing a configuration of a KMS (Key Management Server) included in a system for managing a public key according to an embodiment of the present invention. Fig. 2 is a block diagram showing a configuration of a host having a function as a DNS client. The KMS is a server having an expanded function of the DNS server. Likewise, the host has a function as the function-expanded DNS client. Fig. 3 shows the composition of the table for describing the correspondence between the public key and the domain name. Fig. 4 is a flowchart for describing the routine in which the DNS server answers the public key when it receives an inquiry of the public key. Fig. 5 is a flowchart for describing the routine in which the electronic signature is added to the packet for answering the public key when the DNS server receives an inquiry of the electronic signature. Fig. 6 is a flowchart for describing the routine in which the host having a function of the DNS client acquires the open key of the target host. Fig. 7 is a block diagram showing the application of the invention to the network having the hierarchical structure of the domain name. Fig. 8 is an explanatory view showing the types of packets to be transferred between the host and the EMS and between the EMS and the KMS and the electronic signatures added thereto. Fig. 9 is an explanatory view showing the composition of the format of the DNS packet. Fig. 10 is an explanatory view showing the composition of the format of a resource record contained in the DNS packet. In the Figs. ~~1, 2, 7 and 8~~, ~~a numeral~~ numerals 10 and 20 each denotes a KMS.

Numerals 11 and 21 denote network control units. Numerals 12 and 22 denote IP processing units. Numerals 13 and 23 denote TCP/UDP processing units. A numeral 14 denotes an expanded DNS processing unit. A numeral 15 denotes a domain name/IP address table. Numerals 16 and 25 denote domain name/public key/electronic signature table. Numerals 17 and 26 denote initial holding data. A numeral 24 denotes an expanded DNS client. A numeral 27 denotes a security communication processing unit. A numeral 101 denotes a network. Numerals 141 and 241 denote DNS packet separating units. A numeral 142 denotes a DNS processing unit. A numeral 143 denotes a public key inquiry/answering unit. A numeral 144 denotes an electronic signature processing unit. A numeral 242 denotes a domain name resolver. A numeral 243 denotes a public key inquiry processor. A numeral 244 denotes an electronic signature processing unit. Numerals 71 and 75 denote hosts A and B. Numerals 72 to 74 and 76 denote KMS's.

Page 12, line 22 through page 13, line 9:

In the network system shown in Fig. 7, the network has a hierarchical structure, each hierarchy layer of which is given a domain name. Each layer with its own domain has one KMS. Herein, consider that the host A71 acquires the public key of the host ~~B75~~ B 75. In this case, the host ~~A71~~ A 71 inquires the KMS1 (72) located in the hierarchy of the same domain of the public key of the host ~~B75~~ B 75. At this time, merely by receiving the data of the public key of the host ~~B75~~ B 75, it is impossible to prevent a malignant host from being feigned to be the host ~~B75~~ B 75.

Hence, the host ~~A71~~ A 71 requests the electronic signature of the KMS to be trusted. The KMS trusted by the host ~~A71~~ A 71 is made to be the ~~KMS 00~~ KMS00 (74). Further, the public key of the KMS00 (74) is known to the host ~~A71~~ A 71 as well as the other hosts and is authenticated to all the hosts.

a2

[Page 13, line 10-24:]

When the host ~~A71~~ A 71 requests the data on the public key of the host ~~B75~~ B 75, if the KMS1 (72) has the key on the public key of the host ~~B75~~ B 75 in response to this request, the ~~KMS 00~~ KMS00 (74) trusted by the host ~~A71~~ A 71 is requested to add the electronic signature to the data on the public key. On the other hand, if the KMS1 (72) does not have the data on the public key of the host ~~B75~~ B 75, the KMS1 (72) inquires the upper KMS0 (73). In this case, the inquiry to the upper KMS is recursively continued until the KMS1 (72) reaches the KMS having the data on the public key of the host ~~B75~~ B 75. The KMS having the data on the public key of the host ~~B75~~ B 75 serves to request the KMS00 (74) to add the electronic signature in response to the inquiry from the KMS1 (72).

[Page 13, line 25 through page 14, line 4:]

The KMS00 (74) requested to add the electronic signature operates to give back the data on the public key of the host ~~B75~~ B 75 to the KMS1 (72). The KMS1 (72) operates to give back the data on the public key of the host ~~B75~~ B 75 to the host ~~A71~~ A 71. In this case, the host ~~A71~~ A 71 operates to determine if the data is to be trusted because it originally knows the public key of the KMS00 (74).

Q2

[Page 14, lines 5-9:]

The foregoing series of processes make it possible for the host ~~A71~~ A 71 to safely acquire the open key of the host ~~B75~~ B 75. The use of the public key therefore makes it possible to do the security communication with the host ~~B75~~ B 75.

Page 17, line 16 through page 18, line 11:

Q3

The domain Name/Public Key/Electronic Signature Table 16, as shown in Fig. 3, contains a domain name 31, a public key 32, an electronic signature 33 added by the KMS trusted by the host, a KMS name 34 of the KMS having added the signature, and a time stamp 35 for indicating a time point of creating an entry. If an entry is given to the table 16, the public key inquiry/answer processing unit 143 operates to issue a request for an electronic signature to another KMS according to the inquiry request or the electronic signature processing unit 144 operates to add an electronic signature to the answer packets for the public key. If no entry is given to the table, the public key inquiry/answer processing unit 143 operates to transmit the packets for inquiring the public key of the domain name of inquiry to another KMS through the TCP/UDP processing unit 13. The electronic signature processing unit 144 operates to issue a request for an electronic signature to another EMS according to the inquiry request or add an electronic signature to the answer packets of the public key when the unit 144 receives the request for an electronic signature from another KMS in the format of the expanded KMS packet from the TCP/UDP processing unit 13.

Page 18, line 24 through page 19, line 6:

A4

The host 20 is configured to have a network control unit 21, an IP processing unit 22, a TCP/UDP processing unit 23, an expanded DNS client 24, a domain name/public key/electronic signature table 25, initial holding data 26, and a security communication processing unit 27 and is connected to the IP network ~~101~~ 201 through the network control unit ~~11~~ 21. The expanded DNS client 24 is made up of a DNS packet separating unit 241, a domain name resolver 242, a public key inquiry processing unit 243, and an electronic signature check unit 244.

Page ~~21~~, lines 15-26:

A5

In Fig. 7, KMS0 (73), KMS1 (72), KMS2 (76), and KMS00 (74) are the KMS having the structure described with reference to Fig. 1. The hosts ~~A71~~ A 71 and ~~B75~~ B 75 are the hosts having a function of the expanded DNS client having the configuration shown in Fig. 2. Then, the KMS00 (74) is connected to the network 701 having a domain name xx. The KMS0 (73) is connected to the network 702 having a domain name a.xx. The hosts ~~A71~~ A 71 and KMS1 (72) are connected to the network ~~73~~ 703 having a domain name b.a.xx. The ~~host B75~~ hosts B 75 and the KMS2 (76) are connected to the network 704 having a domain name c.a.xx.

Page 21, line 27 through page 22, line 12:

The domain name has a hierarchical structure, in which each KMS is served as the conventional DNS server. Fig. 8 shows the operation of each KMS if only the KMS2 (76) has the information on the public key of the host ~~B75~~ B 75. Each arrow

a5 shown in Fig. 8 shows the packets to be transferred between the host and the KMS and between the KMS and the KMS and the format of the electronic signature to be added to the packet when the host ~~A71~~ A 71 obtains the public key of the host ~~B75~~ B 75. The types of the packets include a public key inquiry, an electronic signature request, and a public key answer.

Page 22, lines 21-23:

a6 Later, the flow of Fig. 4 will be described on the assumption that the KMS whose electronic signature is requested by the host ~~A71~~ A 71 is KMS00 (74).

Page 22, line 24 through page 23, line 16:

(1) At first, the host A operates to transmit 25 the packet for inquiring the public key of the host ~~B75~~ B 75 to the KMS1 (72). As indicated by an arrow 81 in Fig. 8, the packet for inquiring this public key is as follows.

$$S(T(A), [D(B), KMS(A), IP(A), D(A)])$$

As will be understood from the foregoing definition, the electronic signature is given by the secret key of the host A to the message made up of the domain name of the host B, the KMS whose electronic signature is requested by the host A, the 12 address of the host A, and the domain name of the host A. When the KMS1 (72) receives the packet for inquiring the public key of the host ~~B75~~ B 75 from the host ~~A71~~ A 71, the electronic signature processing unit 144 shown in Fig. 1 operates to check the electronic signature added to the packet. The electronic signature processing unit 144 operates to pick up the public key of the host ~~A71~~ A 71 from the

Q6

domain name/public key/electronic signature table 16 and determine if the content of the packet is interpolated through the use of the public key (step 41).

Page 23, line 28 through page 24, line 12:

Q7

(3) If no entry is found in the domain name/public key/electronic signature table 16 in the determination at the step 42, the public key inquiry/answer processing unit 143 of the KMS1 (72) shown in Fig. 7 determines if the domain name of the host of inquiry is matched to the name of the network to which the host belongs and the domain name of the KMS1 (72) is matched to the name of the network to which the KMS1 (72) belongs. For example, in Fig. 7, if the host of inquiry is ~~B75~~ B 75, the domain name c.a.xx of the network to which ~~B75~~ B 75 belongs does not coincide with the domain name b.a.xx of the network to which KMS1 (72) belongs (step 44).

Page 24, line ~~26~~ through page 27, line 7:

Q8

(5) If the names of the networks do not coincide with each other in the determination at the step 44, the KMS1 (72) operates to check the inquiring destination by referring to the domain name 172 of the upper KMS held in the initial holding data 17 in Fig. 1 and then inquire the KMS0 (73) of the public key of the host ~~B75~~ B 75. The inquiring packet is, as shown by an arrow 82 in Fig. 8, as follows.

S(T(KMS1), [D(B), KMS(A), IP(KMS1), D(KMS1)])

The message is made up of the domain name of the host ~~B75~~ B 75, the domain name of the EMS whose electronic signature is requested by the host ~~A71~~ A 71, the IP address of the KMS1 (72), and the domain name of the KMS1 (72) with addition of

a8 an electronic signature whose key is the secret key of the KMS1 (72). The addition of the electronic signature serves to prevent malignant interpolation of the inquiring packet by adding the electronic signature (step 46).

Page ~~26~~, lines 20-24:

a9 (11) If an entry is added to the electronic signature of the specified KMS in the check at the step 47, the public key inquiry/answer processing unit 143 gives the public key with the electronic signature in the entry back to the host ~~A71~~ A 71 (step 48).

[Page 26, line 25 through page 27, line 11:]

(12) On the other hand, if the entry has no electronic signature of the specified KMS at the step 47, the public key inquiry/answer processing unit 143 operates to check the KMS trusted by the host A 71 and added to the packet and the domain name 172 of the upper KMS of the initial holding data shown in Fig. 1. Then, the unit 143 operates to issue a request for an electronic signature to the EMSO (73) shown in Fig. 7 (arrow 83, Fig. 8).

If the KMS2 (76) has information on the public key of the host ~~B75~~ B 75 and issues a request for an electronic signature to the KMS0 (73), as shown by an arrow 84 in Fig. 8, with [D(B), KMS(A), IP(KMS1), S(B) and D(KMS2)] as a message, the request with the electronic signature whose key is a secret key of KMS2 (76) is given (step 49).

Page 28, line 16 through page 29, line 1:

(4) In the determination at the step 52, if the request for the electronic signature is not directed for the KMS0 (73), the electronic signature processing unit 144 operates to refer to the domain name 172 of the upper KMS in the initial holding data and then issue the request for an electronic signature to the upper KMS. In Fig. 7, if the KMS whose electronic signature is requested by the host ~~A71~~ A 71 is KMS00 (74), as shown by an arrow 85 in Fig. 8, the packet for requesting an electronic signature given from the KMS0 (73) to the KMS00 (74) has an electronic signature whose key is the secret key of the KMS0 (73) with [D(B), KMS(A), IP(KMS1), S(B) and D(KMS0)] as a message (step 54).

Page ~~29~~, lines 18-24:

(1) In Fig. 7, it is assumed that the host ~~A71~~ A 71 tries to acquire the open key of the host ~~B75~~ B 75. At this time, the open key inquiry processing unit 243 of the host ~~A71~~ A 71 having the configuration shown in Fig. 2 operates to retrieve the domain name/public key/electronic signature table 25 for checking if any entry to the host ~~B75~~ B 75 is given (step 61).

Page 29, line 25 through page 30, line 6:

(2) At the step 61, if no entry to the host ~~B75~~ B 75 is found in the domain name/public key/electronic signature table 25, the public key inquiry processing unit 243 operates to refer to the domain name/public key 263 of the trusted KMS in the initial holding data 26 for selecting the trusted KMS. If two or more domain

A11

name/public keys 263 of the trusted KMS are found, the unit 243 operates to select the KMS that is upper than and closest to the domain name of inquiry (step 62).

Page 30, lines 7-14:

(3) Next, the public key inquiry processing unit 243 operates to refer to the domain name 262 of the KMS for inquiring the pubic key in the initial hold data 26, for inquiring the KMS of the hold ~~B75~~ B 75. The packet for inquiring the public key includes an electronic signature with [D(B), KMS(A), IP(A) and D(A)] as a message and the secret key T(A) of the old A as a key (step 63).

Page 30, lines 15-21:

(4) When the public key answer packet is given back in response to the inquiry at step 63, the host ~~A71~~ A 71 operates the electronic signature check unit 244 shown in Fig. 2 and then checks if the electronic signature added to the public key answer packet is given by the requested KMS and the content of the packet is interpolated (step 64).

Page 30, line 22 through page 31, line 4:

(5) If the public key answer packet is not given back within a certain interval of time or it is checked that at the step 64 the electronic signature added to the public key answer packet is given by the requested KMS and the content of the packet is interpolated, the host ~~A71~~ A 71 terminates the process without taking any action. This makes it possible to prevent a malignant host from being feigned to be a target

A11

host of the security communication by pretending its own public key and address to correspond with the inquired domain name.

Page ~~31~~, lines 15-19:

(7) The security communication processing unit 276 of the host ~~A71~~ A 71 operates to start the process for the security communication through the use of the public key acquired by the foregoing process or the public key found at the step 61 (step 66).

A12